# Reading List

## 1 Traffic Analysis

- D. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, v. 24, n. 2, February 1981, pp. 84-88.
- E. Gabber, P. Gibbons, Y. Matias, and A. Mayer. "How to Make Personalized Web Browsing Simple, Secure, and Anonymous," *Financial Cryptography '97*, February 1997.
- C. Gülcü and G. Tsudik. "Mixing Email with *Babel*," *1996 Symposium on Network and Distributed System Security*, San Diego, February 1996.
- A. Pfitzmann, B. Pfitzmann, and M. Waidner. "ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead," *GI/ITG Conference: Communication in Distributed Systems*, Informatik-Fachberichte 267, Springer-Verlag, Heidelberg, 1991, pp. 451-463.
- A. Pfitzmann, M. Waidner. "Networks Without User Observability - Design Options," *Advances in Cryptology - EUROCRYPT '85*, Springer LNCS 219.

## 2 Cryptography

- National Bureau of Standards, NBS FIPS PUB 46, "Data Encryption Standard," US Department of Commerce, 1977.
- R. Rivest, A. Shamir, L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, v. 21, n. 2, February 1978, pp. 120-126.
- J. Moore. "Protocol Failures in Cryptosystems," *Proceedings of the IEEE*, v. 76, n. 5, May 1988.
- P. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other System," *Advances in Cryptology - CRYPTO '96*, Springer LNCS 1109.
- B. Pfitzmann, A. Pfitzmann. "How to Break the Direct RSA-Implementation of MIXes," *Advances in Cryptology - EUROCRYPT '89*, Springer LNCS 434.

# 3 Networks / Routing

- R. Perlman. "Interconnections: Bridges and Routers," Addison-Wesley Publishing Company, Inc., Chapter 11, 1992. (Summary of R. Perlman. "Network Layer Protocols with Byzantine Robustness," Ph.D. dissertation, MIT, 1988.)
- R. Braden (ed). "Requirements for Internet Hosts - Communication Layers," RFC 1122, May 1989.
- G. Malkin (ed). "RIP Version 2: Carrying Additional Information," RFC 1723, November 1994.
- J. Moy (ed). "OSPF Version 2," RFC 2328, April 1998.
- Y. Rekhter, T. Li (ed). "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, March 1995.